UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,409	12/04/2003	Richard C. Johnson	021756-087310US	7705

51206 7590 10/19/2009

TOWNSEND AND TOWNSEND AND CREW LLP
TWO EMBARCADERO CENTER
8TH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
AGWUMEZIE, CHARLES C	
ART UNIT	**PAPER NUMBER**
3685	

MAIL DATE	DELIVERY MODE
10/19/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/727,409	JOHNSON, RICHARD C.	
	Examiner	Art Unit	
	CHARLES C. AGWUMEZIE	3685	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 August 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *9-13,15-19 and 29-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9-13, 15-19and 29-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

12/4/03; 12/17/03; 8/15/05; and 05/09/07

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on August 10, 2009 has been entered.

Acknowledgment

2. Applicant's amendment filed on August 10, 2009 is acknowledged. Accordingly claims 9-13, 15-19 and 29-33, remain pending.

Response to Arguments

3. Applicant's arguments filed on August 10, 2009 have been fully considered but they are not persuasive.

4. With respect to **claim 9,** Applicant argues that Brown, Tallent, and Hwangbo, either individually or in combination, fail to disclose one or more of the claim limitations recited in each of claims 9-13, 15-19 and 29-33. Specifically that neither Brown, Tallent, and Hwangbo discloses (1) comparing the retrieved authority information with the authority information included within the received certificate to determine whether the retrieved authority information matches the authority information included within the

received certificate; (2) the store of authority information that is coupled to the network, that is stored apart from the payment request and that is independent of the received certificate; and (3) the authority information including a maximum payment that the user is authorized to make and an indication of payees to whom the user is authorized to make payments as recited in the amended independent claim 9.

In response, Examiner respectfully disagrees with Applicant's characterization and submits that Brown, Tallent, and Hwangbo, either individually or in combination does disclose the claimed limitations.

For example and with respect to (1) above Brown discloses that if a match is found, the signer is authorized for the corresponding role (0088). Brown further discloses that when a match is found, the corresponding private key is retrieved from the database (0089). Brown also discloses that the recipient calculates a new message digest for the message and compares it with the original message digest…(0015; 0072). Thus Brown does disclose comparing the retrieved authority information with the authority information included within the received certificate to determine whether the retrieved authority information matches the authority information included within the received certificate.

With respect to (2) above Tallent clearly discloses that the authority is forwarded and verified by the root entity where authority to sign is stored (see see figs. 1, 4C, 4D, 4E, 5,) and that the Root entity 110 is also preferably provided with a central repository 260 which is preferably adapted to store data…; (0033; 0141-0148, 0167). From the above it is evident that the authority to sign database is stored in the central repository

which is apart from the received payment request and independent of the received certificate. Accordingly Tallent does disclose that the store of authority information that is coupled to the network, that is stored apart from the payment request and that is independent of the received certificate.

With respect to (3) above Brown clearly discloses …the maximum signing authority of the signer…the digital certificate may specify a maximum signing authority… for example, a signer may only be authorized to digitally sign requests up to $1000.00. Thus, the digital certificate of the signer will indicate a maximum signing authority of $1000.00 (see fig. 8G, which discloses check certificate for maximum signing authority of the signer step 886; amount authorized step 888; 0183). Accordingly Brown does disclose the authority information including a maximum payment that the user is authorized to make and an indication of payees to whom the user is authorized to make payments as recited in the amended independent claim 9.

5. With respect to **claims 15 and 29**, Applicant argues that these claims are allowable for at least a similar rationale as discussed for allowability of claim 9.

In response, Examiner respectfully disagrees and submits that claims 15 and 29 are not allowable for at least the reasons given above with respect to claim 9.

6. With respect to dependent **claims 10-13, 16-19, and 30-33**, Applicant argues that these claims depend directly or indirectly from claims 9, 15 and 29 respectively and are therefore allowable for at least the same rationale as discussed for the allowability of claim 9.

In response, Examiner respectfully disagrees and submits that these claims are not allowable either by virtue of their dependency from claims 9, 15 and 29 and/or for their own individually recited features.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 9-13, and 15-19,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Brown et al U.S. Patent Application Publication No. 2004/0139327 A1 in view of Tallent JR. et al (hereinafter "Tallent") U.S. Patent Application Publication No. 2006/0179008 A1.

9. As per **claim 9**, Brown et al discloses a computer-implemented method for ensuring non-repudiation of a payment request, the payment request being generated in a computing environment having a connection to a network, the method comprising the steps of:

receiving, over the network, the payment request together with a certificate identifying a user having caused the payment request to be generated, the certificate including certificate-identifying information and user-identifying information, the

certificate further including authority information defining an authority of the user to make the payment request (fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80);

the authority information including a maximum payment that the user is authorized to make and an indication of payees to whom the user is authorized to make payments (0183, which discloses …the maximum signing authority of the signer…the digital certificate may specify a maximum signing authority… for example, a signer may only be authorized to digitally sign requests up to $1000.00. Thus, the digital certificate of the signer will indicate a maximum signing authority of $1000.00);

validating the certificate-identifying information and the user-identifying information included within the received certificate by accessing a store of authority information that is independent of the received certificate (figs. 1, 2, 3, and 8; 0165; 0067; 0174; 0183; claim 80);

accessing a store of authority information that is coupled to the network, that is stored apart from the payment request and that is independent of the received certificate;

retrieving from the accessed store of authority information stored authority information that is associated with the user (0088, which discloses that the signer may provide a pass phrase or the like to the role identifier 104, after which the pass phrase is compared against a database of pass phrases for various signing roles…);

comparing the retrieved authority information with the authority information included within the received certificate to determine whether the retrieved authority information matches the authority information included within the received certificate

(0088, which discloses that if a match is found, the signer is authorized for the corresponding role; 0089, which discloses when a match is found, the corresponding private key is retrieved from the database; 0015, which discloses that the recipient calculates a new message digest for the message and compares it with the original message digest…);

validating the authority information within the received certificate only if the retrieved authority information matches the authority information included within the received certificate (0088 which discloses that if a match is found, the signer is authorized for the corresponding role), and

executing of the payment request only when the certificate-identifying information, the user-identifying information and the authority information within the received certificate is successfully validated (0169, which discloses that the certificate includes at least the signer's name and public key…after the certificate is decrypted, the method continues by determining whether the signer's identity … matches the signer's name in the decrypted certificate, if not the signature verification service 710 terminates with the signature not being verified…see claim 49, which discloses completing the electronic payment request when the payment amount does not exceed the signer's maximum authority; se also fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80).

10. What Brown does not explicitly teach is:

accessing a store of authority information that is coupled to the network, that is stored apart from the payment request and that is independent of the received certificate;

11. Tallent discloses accessing a store of authority information that is coupled to the network, that is stored apart from the payment request and that is independent of the received certificate (see figs. 1, 4C, 4D, 4E, 5, where authority is forwarded and verified by the root entity where authority to sign is stored; 0033, which discloses that Root entity 110 is also preferably provided with a central repository 260. Central repository 260 is preferably adapted to store data…; 0141-0148, 0167).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the system of Brown et al and incorporate a method comprising accessing a store of authority information that is coupled to the network, that is stored apart from the payment request and that is independent of the received certificate in view of the teachings of Tallent, since the claimed invention is merely a combination of old and known elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable. In addition it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the system of Brown et al and incorporate a method comprising accessing a store of authority information that is coupled to the network, that is stored apart from the payment request and that is independent of the received certificate in order to ensure adequate security of the document.

12. As per **claim 10**, Brown et al further discloses the method, wherein the payment request is for a predetermined amount and wherein the payment request is authorized

only when the validating steps are successful and when the authority information for the user stored in the hierarchical authority data structure lists an authorized amount for the user at least equal to the predetermined amount (0177; 0183; 0184; 0185).

13. As per **claim 11 and 16**, Brown et al further discloses the method, wherein the certificate received in the receiving step conforms to the X.509 standard (0109; 0164; 0183).

14. As per **claim 12 and 17**, Brown et al further discloses the method, wherein the authority information is configured as XML code (0062; 0068; 0069).

15. As per **claim 13 and 18**, Brown et al further discloses the method, wherein the XML code is compliant with a DSML standard (0062; 0068; 0069).

16. As per **claim 15**, Brown et al discloses a computer-readable storage medium configured to store one or more software application configured to carry out a financial transaction, the application being configured to run on a computer coupled to a network, the computer readable storage medium comprising:

certificate receiving code which is configured to receive a digital certificate from a user over the network, the certificate including certificate-identifying information and user-identifying information, the certificate further including authority information that

defines an authority granted to the user to request that the financial transaction be carried out (fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80);

the authority information including a maximum payment that the user is authorized to make and an indication of payees to whom the user is authorized to make payments (0183, which discloses …the maximum signing authority of the signer…the digital certificate may specify a maximum signing authority… for example, a signer may only be authorized to digitally sign requests up to $1000.00. Thus, the digital certificate of the signer will indicate a maximum signing authority of $1000.00);

certificate validating code configured to enable validation of the certificate-identifying information and user-identifying information within the received certificate (fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80) and

authorization validating code configured to cause the computer to carry out steps of:

accessing a store of authority information that is coupled to the network, that is stored apart from the payment request and that is independent of the received certificate;

retrieving from the accessed data structure stored authority information that is associated with the user (0088, which discloses that the signer may provide a pass phrase or the like to the role identifier 104, after which the pass phrase is compared against a database of pass phrases for various signing roles…);

comparing the retrieved authority information with the authority information included within the received certificate to determine whether the retrieved authority

information matches the authority information included within the received certificate (0088, which discloses that if a match is found, the signer is authorized for the corresponding role; 0089, which discloses when a match is found, the corresponding private key is retrieved from the database);

validating the authority information within the received certificate only if the retrieved authority information matches the authority information included within the received certificate (0088 which discloses that if a match is found, the signer is authorized for the corresponding role), and

executing of the financial transaction only when the authority information within the received certificate is successfully validated (0169, which discloses that the certificate includes at least the signer's name and public key…after the certificate is decrypted, the method continues by determining whether the signer's identity … matches the signer's name in the decrypted certificate, if not the signature verification service 710 terminates with the signature not being verified…see claim 49, which discloses completing the electronic payment request when the payment amount does not exceed the signer's maximum authority; se also fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80).

17. What Brown does not explicitly teach is:

accessing a store of authority information that is coupled to the network, that is stored apart from the payment request and that is independent of the received certificate.

18. Tallent discloses accessing a store of authority information that is coupled to the network, that is stored apart from the payment request and that is independent of the received certificate (see figs. 1, 4C, 4D, 4E, 5, where authority is forwarded and verified by the root entity where authority to sign is stored; 0141-0148, 0167).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the system of Brown et al and incorporate a method comprising accessing a store of authority information that is coupled to the network, that is stored apart from the payment request and that is independent of the received certificate in view of the teachings of Tallent in oreder to ensure adequate security of the document.

19. As per **claim 19**, Brown et al further discloses the computer-readable storage medium, wherein the authority defined by the authority information within the received certificate also defines rights of the user to access predetermined data and programs within the network (0183; 0184).

20. **Claims 29-33**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Brown et al U.S. Patent Application Publication No. 2004/0139327 A1 in view of Hwangbo U.S. Patent Application Publication No. 2003/0154376 A1 and further in view of Tallent JR. et al (hereinafter "Tallent") U.S. Patent Application Publication No. 2006/0179008 A1.

21. As per **claim 29**, Brown et al discloses in a server computer to authenticate a user of a client computer and to verify that the user is authorized to request that the server computer carry out a requested action, the server computer comprising:

a processor (see fig. 2, CPU 202; see fig. 5); and

a memory coupled to the processor and configured to store a set of instructions that when executed by the processor causes the processor to:

receive a payment request along with a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion, wherein the first code portion of the digital certificate is configured enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and an extension field;

wherein the second code portion of the digital certificate is configured to define an authority of the user of the client computer to request that the server computer carry out the requested action, the second code portion being configured for inclusion within the extension field of the first code portion, the authority of the user defined within the second code portion of the certificate defining access rights of the user (see figs. 1 and 3; 0165; 0067; 0174; 0183), including a maximum payment that the user is authorized to make and an indication of payees to whom the user is authorized to make payments (0183, which discloses …the maximum signing authority of the signer…the digital certificate may specify a maximum signing authority… for example, a signer may only

be authorized to digitally sign requests up to $1000.00. Thus, the digital certificate of the signer will indicate a maximum signing authority of $1000.00);

access a store of authority information that is coupled to the network, that is stored independent of the received digital certificate;

retrieve from the accessed store of authority information stored authority information that is associated with the user (0088, which discloses that the signer may provide a pass phrase or the like to the role identifier 104, after which the pass phrase is compared against a database of pass phrases for various signing roles…);

compare the retrieved authority information with the authority information included within the received certificate to determine whether the retrieved authority information matches the authority information included within the received certificate (0088, which discloses that if a match is found, the signer is authorized for the corresponding role; 0089, which discloses when a match is found, the corresponding private key is retrieved from the database);

validate the authority information within the received certificate only if the retrieved authority information matches the authority information included within the received certificate (0088 which discloses that if a match is found, the signer is authorized for the corresponding role), and

carry out the requested action only when the the authority information within the received certificate is successfully validated (0169, which discloses that the certificate includes at least the signer's name and public key…after the certificate is decrypted, the method continues by determining whether the signer's identity … matches the signer's

name in the decrypted certificate, if not the signature verification service 710 terminates with the signature not being verified…see claim 49, which discloses completing the electronic payment request when the payment amount does not exceed the signer's maximum authority; se also fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80).

22. What Brown does not explicitly teach is:

access a store of authority information that is coupled to the network, that is stored independent of the received digital certificate;

a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion, wherein the first code portion of the digital certificate is configured enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and the extension field (extension fields are inherent in X.509 certificates)

23. Hwangbo discloses a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion, wherein the first code portion of the digital certificate is configured enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and the extension field (fig. 10; 0029; 0034; 0096; claim 17).

24. Tallent discloses access a store of authority information that is coupled to the network, that is stored independent of the received digital certificate (see figs. 1, 4C, 4D,

4E, 5, where authority is forwarded and verified by the root entity where authority to sign is stored; 0141-0148, 0167)

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the system of Brown et al and incorporate a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion, wherein the first code portion of the digital certificate is configured to enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and an extension field and matching the authority of a user within the second code portion of the certificate to corresponding authority information of the user retrieved from the accessed independent store of authority information in view of the teachings of Hwangbo and Tallent respectively in order to ensure adequate security of the document and transaction.

25. As per **claim 30**, Brown further discloses the server computer, wherein the digital certificate conforms to the X.509 standard (0109; 0164; 0183)

26. As per **claim 31** Brown further discloses the server computer wherein the second code portion is configured as XML code (0062; 0068; 0069).

27. As per **claim 32**. Brown further discloses the server computer, wherein the XML code is compliant with a DSML standard (0062; 0068; 0069).

28. As per **claim 33**. Brown further discloses the server computer, wherein the authority of the user of the client computer is stored in a hierarchical authority data structure that is accessible by the server computer (0165 which discloses that the certificates are stored in an online, publicly accessible repository and are accessed using a standard protocol).

Conclusion

29. Any inquiry concerning this communication or earlier communications from the examiner should be directed to **Charles C. Agwumezie** whose number is **(571) 272-6838**. The examiner can normally be reached on Monday – Friday 8:00 am – 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Andrew Fischer** can be reached on **(571) 272 – 6779**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free). If you would like assistance from a USPTO

Customer Service Representative or access to the automated information system, call

800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Charlie C Agwumezie/
Primary Examiner, Art Unit 3685
October 15, 2009